INDONESIA

LAPORAN RESMI

PRIZM

Konsep awal mata uang digital

Revisi Laporan Resmi Prizm — June, 2020

PZM.SPACE

PRIZM

PENGANTAR

Bitcoin adalah mata uang digital pertama di dunia yang terdesentralisasi, memungkinkan Anda menyimpan dan mentransfer koin kriptografi dengan mudah menggunakan jaringan P2P untuk mengirimkan informasi, hashing sebagai sinyal sinkronisasi untuk mencegah pengeluaran ganda, serta sistem skrip yang kuat untuk menentukan pemilik koin. Ini menunjukkan perkembangan teknologi dan infrastruktur bisnis. Menurut desain aslinya, bitcoin dapat dipertukarkan, dan dipandang sebagai alat pertukaran netral. Bitcoin dapat memiliki properti khusus yang didukung oleh Penerbit atau perjanjian publik, dan memiliki nilai yang independen dari nilai nominal yang mendasarinya. Bitcoin telah membuktikan bahwa sistem pembayaran elektronik P2P benar-benar dapat bekerja dan memproses pembayaran tanpa keterlibatan pihak ketiga.

Namun, agar seluruh e-ekonomi didasarkan pada solusi peer-to-peer sepenuhnya terdesentralisasi, sistem harus dapat melakukan hal berikut:

1 - Memproses transaksi dengan aman, cepat dan efisien, dalam jumlah ribuan per jam atau lebih;
2 - Mendorong orang untuk berpartisipasi dalam keamanan jaringan;
3 - Skala di tingkat global dengan konsumsi sumber daya minimum;
4 - Dan untuk dapat bekerja pada berbagai perangkat termasuk ponsel.

PZM (diucapkan sebagai "Prizm") memenuhi semua kondisi ini. Keuntungan lainnya, unik, PARAMINING, yang tidak ada dalam mata uang kripto lainnya.

Tetapi lebih lanjut tentang itu nanti.

P R I Z M

ULASAN

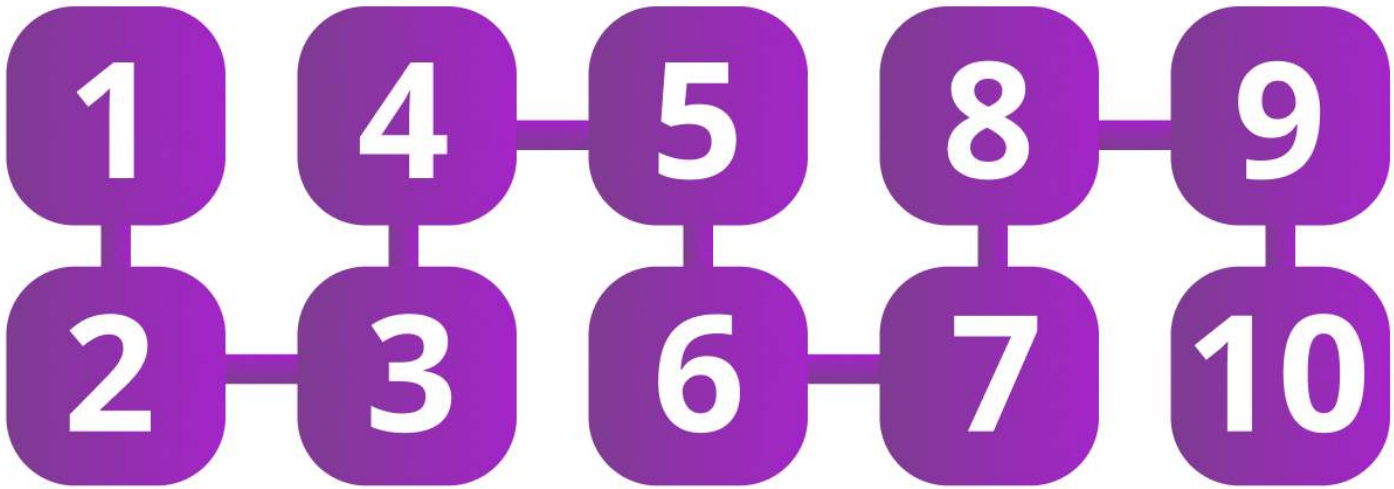
PRIZM - adalah mata uang kripto yang 100% proof-of-stake (menambang dengan menyimpan koin di dompet) berdasarkan NEXT-kernel, yang mana dibangun di Java dengan kode open source. Algoritma PRIZM proof-of-stake yang unik tidak bergantung pada implementasi konsep "usia koin" yang digunakan oleh mata uang kripto proof-of-stake lainnya, dan tahan terhadap serangan "nothing at stake". Jumlah koin yang tersedia didistribusikan di blok Genesis. Kriptografi Curve25519 digunakan untuk memberikan keseimbangan keamanan dan kekuatan pemrosesan yang diperlukan bersama dengan algoritma hashing SHA256 yang lebih umum digunakan.

PRIZM

ULASAN

60detik

Blok dihasilkan setiap 60 detik, rata-rata, berdasarkan akun yang tidak diblokir di node jaringan.



PZM didistribusikan kembali dengan memasukkan biaya transaksi yang diberikan ke akun ketika berhasil membuat blok. Proses ini dikenal sebagai penempaan dan mirip dengan gagasan "penambangan" yang digunakan oleh mata uang kripto lainnya. Transaksi dianggap aman setelah 10 blok konfirmasi , dan arsitektur serta ukuran blok PZM saat ini memungkinkan pemrosesan hingga 367.200 transaksi per hari.

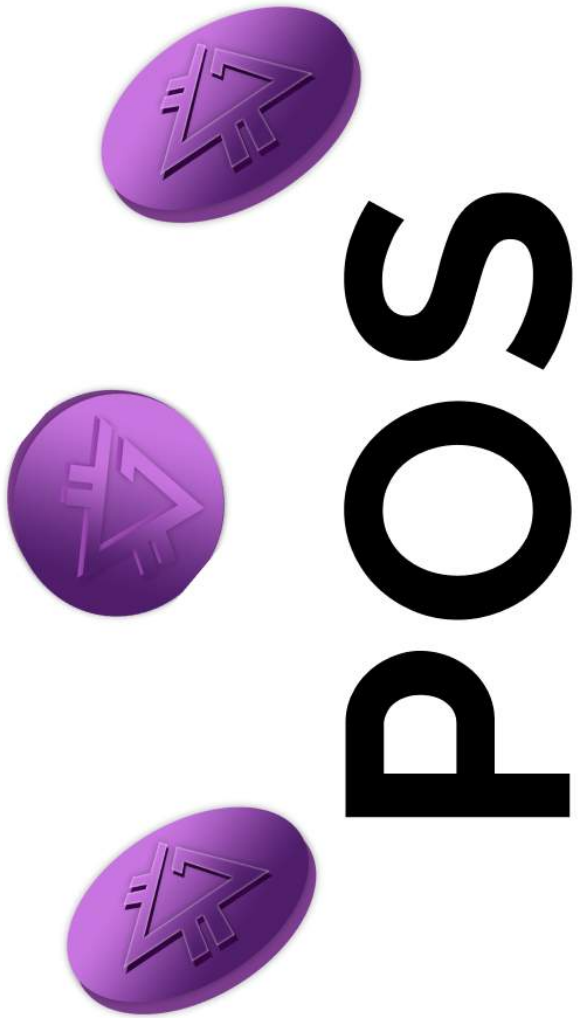
PZM termasuk penerapan Transparent Forging(Penempaan transparan) yang akan memungkinkan Anda untuk meningkatkan kinerja pemrosesan transaksi dua kali lebih besar dengan menggunakan algoritma pembangkitan yang merupakan blok deterministik, dikombinasikan dengan mekanisme keamanan tambahan dari jaringan.

PRIZM

TEKNOLOGI INTI

Proof of Stake

(Menambang dengan menyimpan koin di dompet)



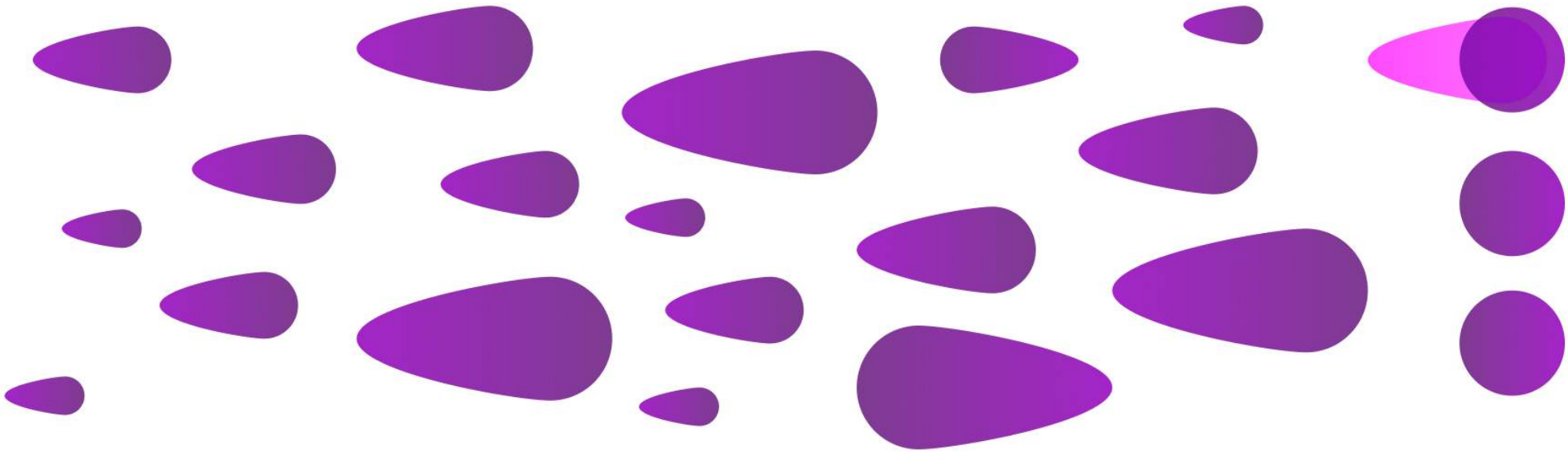
Pada jaman dulu model "Proof of Work" (menambang menggunakan alat) digunakan oleh mayoritas mata uang kripto, keamanan jaringan dipastikan oleh peserta yang melakukan "pekerjaan". Mereka menggunakan sumber daya mereka (perhitungan / waktu pemrosesan) untuk merekonsiliasi transaksi dengan biaya ganda dan untuk membebankan banyak biaya pada mereka yang berusaha untuk menutup transaksi. Untuk pekerjaan ini, peserta diberikan PZM, dan frekuensi serta jumlahnya bervariasi tergantung pada parameter kerja mata uang kripto. Proses ini dikenal sebagai penambangan. Frekuensi pembuatan blok, yang menentukan setiap hadiah yang tersedia untuk penambang mata uang kripto, sebagai suatu peraturan, harus tetap konstan.

Hasilnya, intensitas tenaga kerja dari pekerjaan yang diperlukan untuk mendapatkan hadiah harus meningkat karena jaringan menjadi lebih efisien. Ketika jaringan Proof of Work(menambang menggunakan alat) berkembang, pengguna memiliki lebih sedikit bonus untuk mendukung jaringan, karena potensi bonus mereka didistribusikan ke lebih banyak rekan bisnis. Dalam pencarian keuntungan, penambang terus menginvestasikan sumber daya dalam bentuk peralatan khusus dan dipatenkan yang membutuhkan investasi signifikan dan biaya yang dikeluarkan tinggi. Seiring waktu, jaringan menjadi lebih tersentralisasi karena mitra yang lebih sedikit (mereka yang melakukan lebih sedikit pekerjaan) keluar atau menyatukan sumber daya mereka ke dalam kolam tambang. Pencipta bitcoin Satoshi Nakamoto, yang dimaksud agar jaringan bitcoin sepenuhnya terdesentralisasi. Tetapi tidak ada yang bisa memprediksi bahwa bonus yang diberikan oleh sistem Proof of Work akan mengarah pada sentralisasi proses penambangan. Ini mengarah pada potensi kerentanan.

PRIZM

PROOF OF STAKE (MENAMBANG DENGAN MENYIMPAN KOIN DI DOMPET)

TEKNOLOGI INTI



GHash. Kolam penambangan bitcoin IO telah mencapai 51% dari kekuatan penambangan bitcoin di masa lalu, dan lima kolam penambangan bitcoin teratas merupakan 70% dari kekuatan jaringan hashing. Konsep desentralisasi beresiko kerugian total. Model Proof of Stake(menambang dengan menyimpan koin di dompet) digunakan oleh Prizm, keamanan jaringan diatur oleh mitra yang memiliki kepentingan dalam jaringan.

Insentif yang diberikan oleh algoritma ini tidak kondusif untuk sentralisasi sebagai algoritma Proof of Work(menambang menggunakan alat), dan data menunjukkan bahwa jaringan Prizm sangat terdesentralisasi sejak awal: sejumlah besar (dan terus bertambah) jumlah akun unik memberikan kontribusi blok ke jaringan, dan lima akun teratas menghasilkan 35% dari total jumlah blok.

PRIZM

PROOF OF STAKE (MENAMBANG DENGAN MENYIMPAN KOIN) DALAM PRIZM

Prizm menggunakan sistem di mana setiap "koin" dalam akun dapat dianggap sebagai ladang pertambangan. Semakin banyak koin yang ada dalam akun, semakin besar kemungkinan akun tersebut akan menerima hak untuk membuat blok. Total "hadiah" yang diterima sebagai hasil dari menciptakan blok, jumlah komisi untuk transaksi terletak di dalam blok. PRIZM tidak membuat koin baru apa pun sebagai hasil dari membuat blok. PRIZM tidak membuat koin baru sebagai hasil dari membangun blok. Pembagian PZM terjadi sebagai hasil dari pembuatan blok yang menerima biaya transaksi, sehingga istilah "penempaan" digunakan dalam konteks ini sebagai ganti “menambang” dan berarti untuk "membuat hubungan atau kondisi baru". Blok berikutnya dihasilkan berdasarkan informasi yang dapat diverifikasi, unik, dan hampir tidak dapat diprediksi dari blok sebelumnya. Blok dihubungkan berdasarkan tautan ini, menciptakan blockchain (dan transaksi) yang dapat ditelusuri kembali di blok Kejadian. Waktu pembuatan blok adalah sekitar 59 detik, tetapi perubahan dalam probabilitas telah mengarah pada fakta bahwa waktu pembuatan rata-rata blok bisa 80 detik, ada interval blok yang lebih lama. Keamanan Blockchain selalu diatur dalam sistem Proof-of-stake(Menambang dengan menyimpan koin pada dompet).

Prinsip-prinsip dasar penerapan pada algoritma Prizm Proof of Stake (menambang dengan menyimpan koin):

- Nilai kompleksitas kumulatif disimpan sebagai parameter di setiap blok, dan setiap blok berikutnya menerima "kompleksitas" baru dari nilai blok sebelumnya. Dalam kasus ambiguitas, jaringan mencapai konsensus dengan memilih blok atau fragmen rantai dengan kompleksitas kumulatif tertinggi.

- "Agar pemegang akun tidak memindahkan dana mereka dari satu akun ke akun lain sebagai cara memanipulasi agar dapat menghasilkan blok, koin harus diam di dalam akun untuk 1.440 blok sebelum mereka dapat berkontribusi pada proses pembuatan blok. Koin yang memenuhi kriteria ini berkontribusi pada saldo akun yang efisien, dan saldo itu digunakan untuk menentukan probabilitas penempaan.

- Untuk mencegah penyerang membuat rantai baru dari blok Genesis, jaringan hanya memungkinkan restrukturisasi rantai 720 blok yang terletak di belakang blok saat ini. Blok apa pun di bawah ambang batas ini harus ditolak. Ambang batas ini dapat dianggap sebagai satu-satunya pos pemeriksaan PZM yang tetap.

- Karena probabilitas sangat rendah bahwa akun mana pun akan mengambil alih manajemen Blockchain dengan membuat rantai bloknya sendiri, transaksi dianggap aman jika dikodekan menjadi blok yaitu terletak 10 blok di belakang blok saat ini.

PRIZM

PERBANDINGAN DENGAN PEERCOIN PROOF OF STAKE(MENAMBANG DENGAN MENYIMPAN KOIN)

Peercoin menggunakan pengaturan usia koin sebagai bagian dari algoritma peluang penambangan. Dalam sistem ini, semakin lama Peercoins Anda berada di akun Anda (hingga 90 hari), semakin banyak kekuatan (usia koin) yang mereka punya untuk membuat blok. Tindakan "Rapat" blok memerlukan pemakaian martabat usia koin, dan jaringan menentukan konsensus dengan memilih rantai dengan total pemakaian usia koin terbesar. Ketika blok Peercoin dipisahkan, pemakaian usia koin dikembalikan ke akun blok asli.

Hasilnya, biaya untuk menyerang jaringan Peercoin rendah, karena pengganggu dapat terus mencoba untuk menghasilkan blok (disebut pengasahan stake) sampai saat itu, sampai mereka berhasil. Peercoin meminimalkan risiko ini dan lainnya dengan menerbitkan pos-pos pemeriksaan blockchain secara terpusat beberapa kali sehari untuk "membekukan" blockchain dan memblokir transaksi. Prizm tidak menggunakan usia koin sebagai bagian dari algoritma penempaan. Perubahan pembuatan blok oleh akun apa pun hanya bergantung pada saldo saat ini (yang merupakan keuntungan dari setiap akun), waktu sejak blok terakhir (yang dibagikan oleh semua akun penempaan) dan nilai target dasar (yang juga umum untuk semua akun).

PRIZM TOKEN

10 JUTA
PZM

EMISI AWAL

6 MILIAR
PZM

EMISI AKHIR

Emisi awal adalah 10 juta PZM dan jumlah akhirnya adalah 6 miliar PZM. Koin diterbitkan dengan penciptaan blok Genesis (blok pertama di blockchain). Paramining diterapkan di semua negara di dunia, dengan biaya nominal, dalam jumlah terbatas, untuk mencapai permulaan Prizm desentralisasi. Jumlah total PZM akan menjadi 6 miliar token. Akun Genesis menghasilkan sinyal anti-koin Paramining (sinyal mengirim koin untuk dompet tertentu) hingga batas 6 miliar PZM.

Keberadaan anti-koin dalam Genesis memiliki beberapa efek samping yang menarik:

Semua token yang dikirim ke akun Genesis dihancurkan secara efektif, karena saldo akun negatif membatalkannya. Fungsi utama Prizm adalah sistem pembayaran tradisional, tetapi diciptakan untuk melakukan lebih banyak lagi. Tujuan komunitas CWT dapat dicapai di bawah kondisi persamaan PZM dengan mata uang utama Fiat.

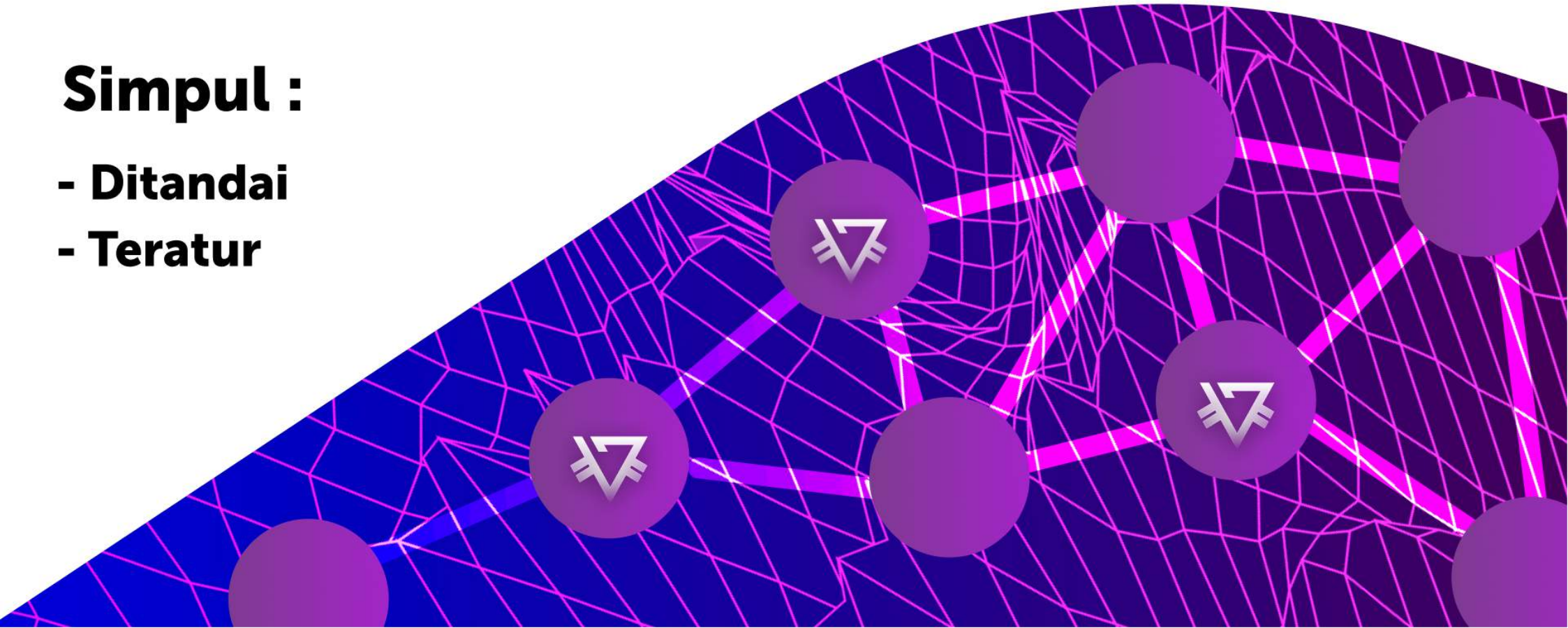
PRIZM

SIMPUL JARINGAN

Simpul jaringan Prizm adalah perangkat apa pun yang melakukan transaksi atau memblokir data ke dalam jaringan. Perangkat apa pun dengan perangkat lunak PZM diperlakukan sebagai simpul. Simpul dapat dibagi menjadi dua jenis: ditandai dan teratur.

Simpul :

- Ditandai
- Teratur



SIMPUL JARINGAN

Simpul yang ditandai hanyalah sebuah simpul yang ditandai dengan token terenkripsi yang diterima dari kunci pribadi akun; token ini dapat membaca sandi untuk menunjukkan alamat akun PZM spesifik dan saldo yang terkait dengan simpul. Tindakan penempatan label pada simpul menambah lapisan akuntabilitas dan kepercayaan, sehingga simpul yang ditandai lebih dapat diandalkan daripada yang tidak memiliki tanda pada jaringan. Semakin banyak saldo akun terhubung ke simpul yang ditandai, semakin besar kepercayaan yang diberikan pada simpul ini. Sementara penyerang mungkin ingin menandai sebuah simpul untuk mendapatkan kepercayaan pada jaringan dan kemudian menggunakan kepercayaan itu untuk tujuan jahat, penghalang untuk masuk (biaya PZM yang dibutuhkan untuk membangun kepercayaan yang memadai) mencegah penyalahgunaan tersebut.

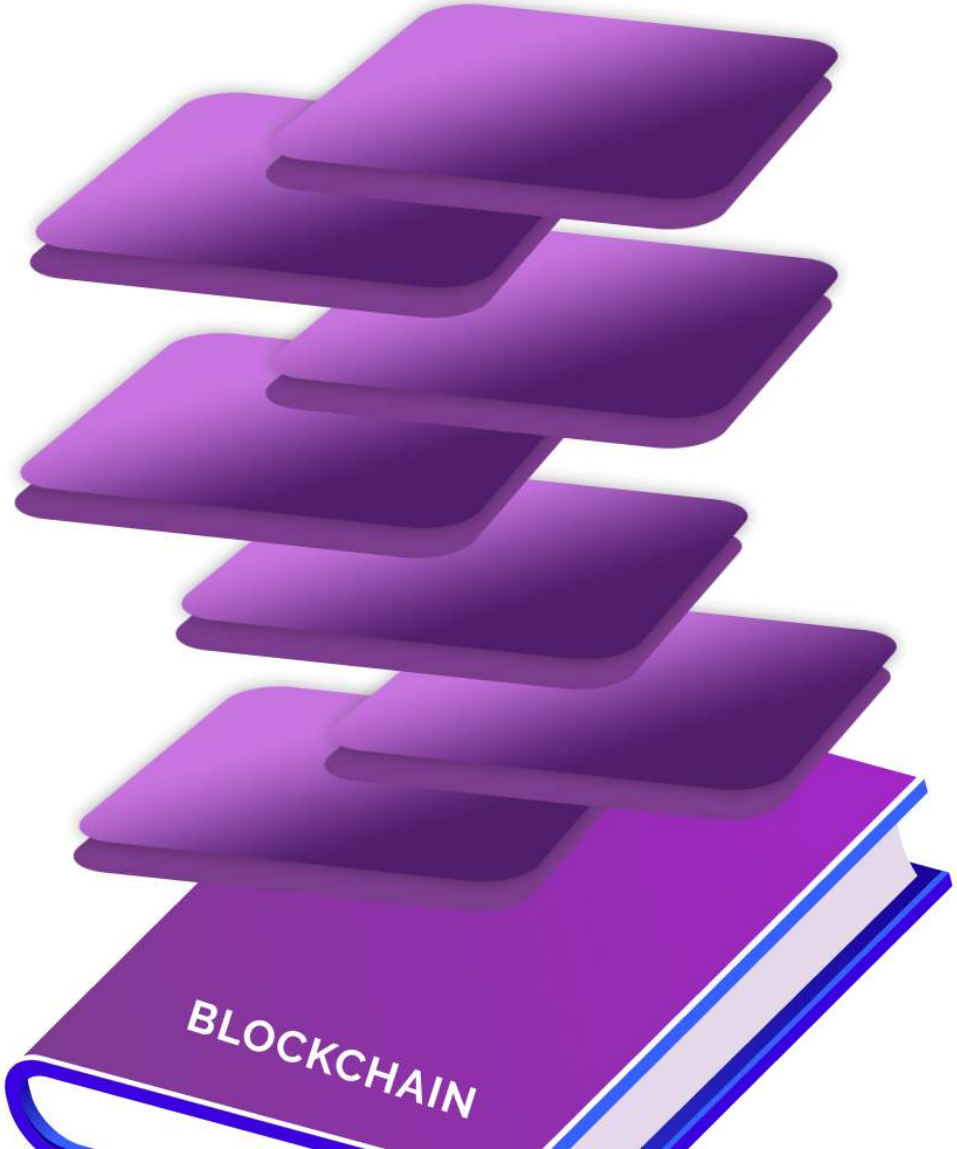
Setiap simpul dalam jaringan PZM memiliki kemampuan untuk memproses dan mentransmisikan transaksi dan memblokir informasi. Blok dipindai karena diterima dari simpul lain, dan dalam kasus di mana pemeriksaan blok tidak dilakukan, simpul dapat "di blacklist" sementara untuk mencegah penyebaran data blok yang tidak valid.

Setiap simpul memiliki mekanisme perlindungan DDOS bawaan (Layanan penolakan distribusi) yang membatasi jumlah permintaan jaringan dari setiap pengguna hingga 30 per detik.

PRIZM

BLOK

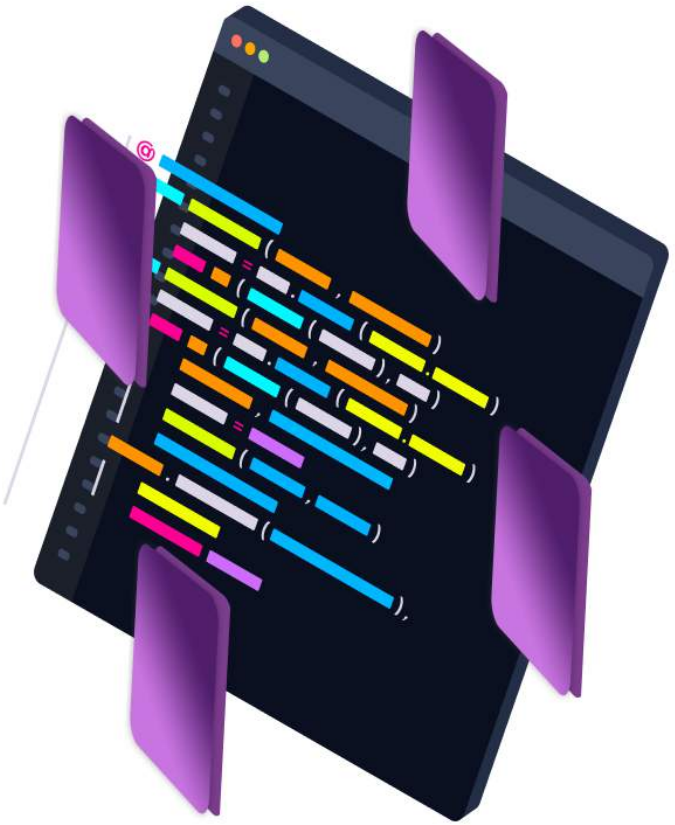
Seperti mata uang kripto lainnya, Buku Besar PZM (Buku Besar transaksi) dibangun dan disimpan dalam serangkaian blok terkait yang dikenal sebagai blockchain. Buku kerja ini menyediakan catatan permanen dari transaksi yang telah terjadi, dan itu juga menetapkan urutan di mana transaksi dilakukan. Salinan Blockchain disimpan pada setiap simpul dalam jaringan Prizm, dan setiap akun yang tidak diblokir pada simpul (dengan memberikan kunci pribadi dari akun ini) memiliki kemampuan untuk menghasilkan blok, asalkan setidaknya satu transaksi masuk di akun telah dikonfirmasi 1.440 kali. Akun apa pun yang memenuhi kriteria ini disebut akun aktif. Dalam PZM, setiap blok berisi hingga 255 transaksi, yang semuanya didahului oleh 192 byte Header yang berisi parameter pengidentifikasi. Setiap transaksi dalam blok diwakili oleh maksimum 160 byte, dan ukuran blok maksimum adalah 32 KB



PRIZM

BLOK

Semua blok berisi parameter berikut:

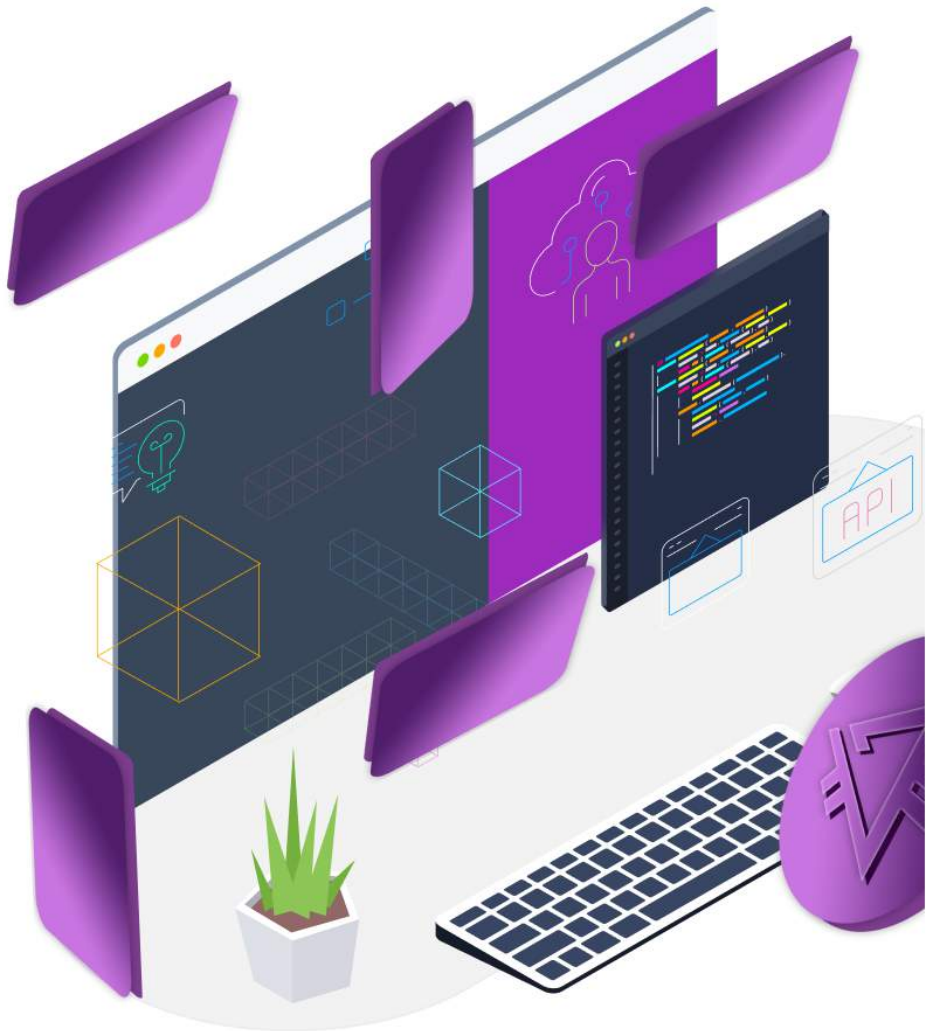


- Versi blok, ketinggian blok dan ID blok
- Waktu blok dinyatakan dalam hitungan detik dari blok Genesis
- ID akun yang membuat blok, serta kunci publik akun.
- ID dan hash dari blok sebelumnya
- Jumlah transaksi yang disimpan di blok
- Jumlah total PZM yang diwakili oleh transaksi dan komisi di blok
- Data transaksi untuk semua transaksi yang termasuk dalam blok, termasuk ID transaksi
- Panjang blok payload dan nilai fungsi hash dari blok payload
- Nilai target dasar dan kesulitan kumulatif untuk blok

PRIZM

PENEMPAAN (PEMBUATAN BLOK)

Ada tiga nilai sebagai kunci untuk menentukan akun mana yang memiliki hak untuk menghasilkan blok, akun mana yang berhak untuk membuat blok dan apa yang dipertimbangkan sebagai otoritatif pada saat konflik: nilai target dasar, nilai target, dan kesulitan kumulatif.



Nilai target dasar

Untuk memenangkan hak untuk menempa (menghasilkan) blok, semua akun Prizm yang aktif "bersaing" dengan mencoba membuat nilai hash yang lebih rendah dari nilai target basis yang ditentukan. Nilai target dasar ini berubah dari blok ke blok dan diturunkan dari nilai target dasar dari blok sebelumnya dikalikan dengan jumlah waktu yang dibutuhkan untuk menghasilkan blok itu.

PRIZM

Nilai target

Setiap акун menghitung nilai targetnya sendiri berdasarkan kurs efektif saat ini.

Nilai ini sama dengan:

$$T = Tb \times S \times Be$$

Dimana :
T - nilai target baru
Tb - nilai target referensi
S - waktu yang telah berlalu sejak blok terakhir dalam detik
Be - saldo akun efektif

Seperti yang Anda lihat dari rumus, nilai target meningkat setiap detik yang telah berlalu sejak blok sebelumnya.

Nilai target maksimum adalah 1.53722867 x 1017, dan nilai target minimum adalah setengah dari nilai target dasar dari blok sebelumnya. Nilai target ini dan nilai target dasar adalah sama untuk semua akun yang mencoba menempa di blok tertentu. Satu-satunya parameter akun yang ditentukan adalah parameter saldo yang efektif.

PRIZM

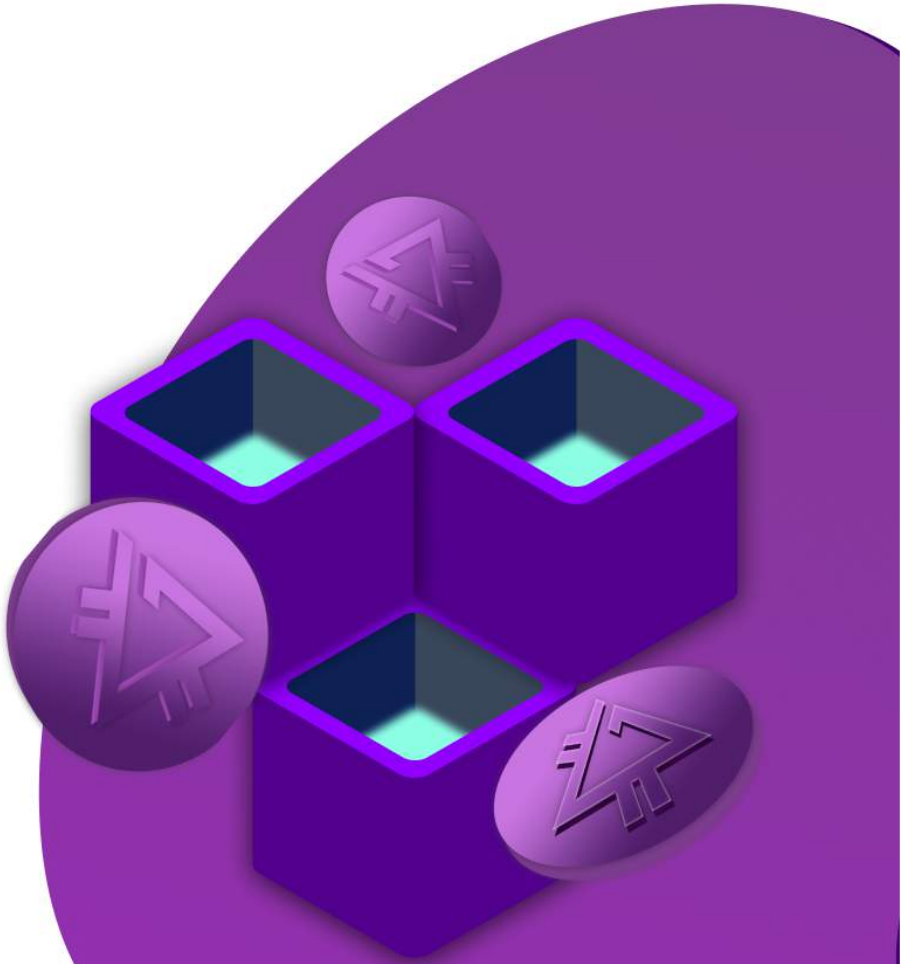
Kompleksitas total

Nilai total kompleksitas yang diperoleh dari nilai target dasar sesuai dengan rumus:

$$Dcb = Dpb + 264 / Tb$$

Dimana :

Dcb - kompleksitas blok saat ini
Dpb - kompleksitas dari blok sebelumnya
Tb - nilai target dasar dari blok saat ini



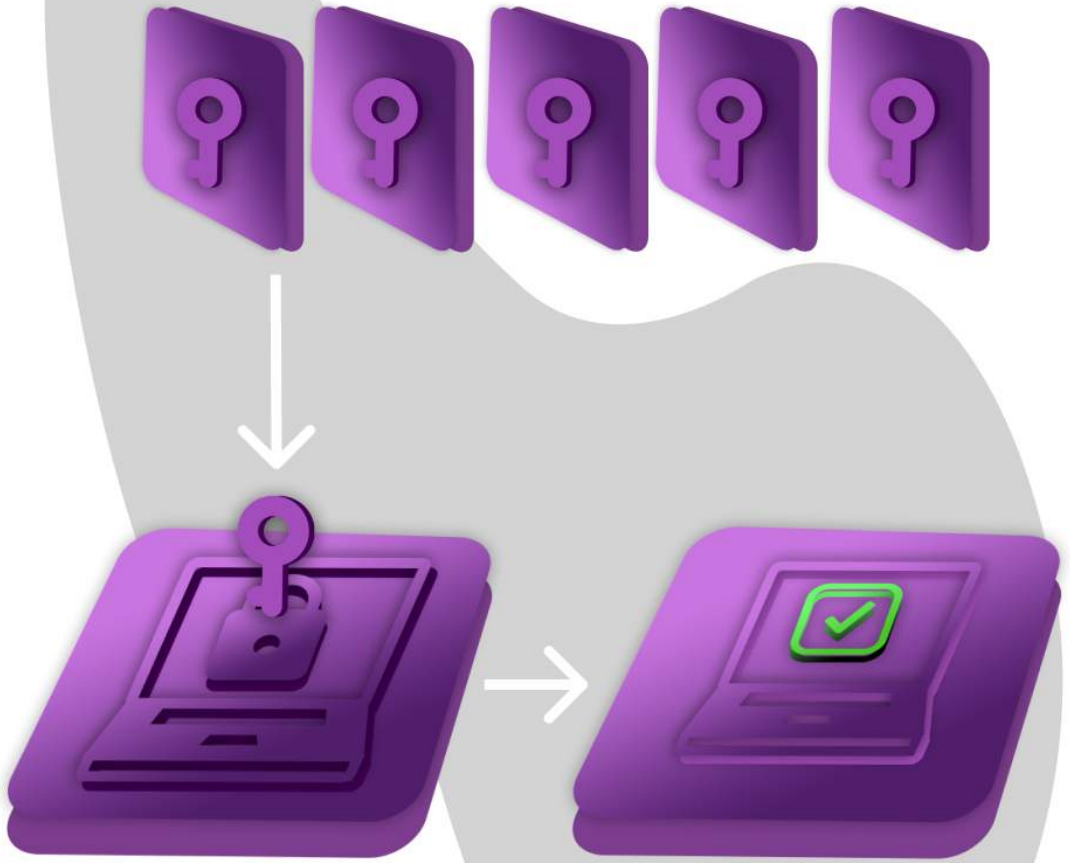
ALGORITMA PENEMPAAN

Setiap blok dalam rantai memiliki parameter generasi bertanda. Untuk berpartisipasi dalam proses penempaan blok, akun aktif secara kriptologis memiliki tanda yaitu blok yang dibuat sebelumnya dengan kunci publiknya sendiri. Ini menciptakan tanda 64-byte yang kemudian di-hash menggunakan SHA256. 8 byte pertama dari hash yang dihasilkan memberikan nomor yang disebut akun hit. Hit dibandingkan dengan nilai target saat ini. Jika hit yang dihitung lebih rendah dari target, blok selanjutnya dapat dihasilkan. Sebagaimana dicatat dalam rumus nilai target, nilai target meningkat setiap detik. Bahkan jika hanya ada beberapa akun aktif di jaringan, salah satunya akan menghasilkan blok karena nilai target akan menjadi sangat besar. Konsekuensi dari ini adalah bahwa Anda dapat memperkirakan waktu yang diperlukan untuk setiap akun untuk mempercepat blok dengan membandingkan nilai hit dari akun itu dengan nilai target. Poin terakhir sangat penting. Karena setiap simpul dapat meminta saldo efektif untuk setiap akun aktif, dimungkinkan untuk menelusuri semua akun aktif untuk menentukan nilai hit masing-masing. Ini berarti bahwa dengan akurasi yang masuk akal, Anda dapat memprediksi apa yang dimenangkan oleh akun berikut untuk memblokir akun palsu. Serangan acak dapat dipicu dengan memindahkan taruhan ke akun yang akan menghasilkan blok berikutnya, yang merupakan alasan lain mengapa taruhan PZM harus 1.440 blok sebelum dapat berkontribusi pada penempaan (melalui nilai saldo yang efektif). Yang menarik, target basis baru untuk blok berikutnya tidak dapat diprediksi secara wajar, sehingga proses deterministik untuk menentukan siapa yang akan mempercepat blok berikutnya menjadi lebih dan lebih stokastik karena upaya dilakukan untuk memprediksi blok di masa depan.

P R I Z M

ALGORITMA PENEMPAAN

Fitur dari algoritma PRIZM penempaan ini membantu membentuk dasar untuk pengembangan dan implementasi algoritma Penempaan Transparan. Ketika akun aktif diberikan hak untuk membuat blok, itu menggabungkan hingga 255 transaksi yang belum dikonfirmasi yang tersedia ke dalam blok baru dan mengisi blok dengan semua parameter yang diperlukan. Blok ini kemudian ditransmisikan ke jaringan sebagai kandidat Blockchain. Payload yang menghasilkan akun dan semua tanda di setiap blok dapat diperiksa oleh semua simpul jaringan yang menerimanya. Dalam situasi di mana beberapa blok dihasilkan, simpul akan memilih blok dengan kompleksitas akumulasi tertinggi sebagai blok otoritatif. Karena data blok didistribusikan di antara anggota (rekan-rekan), fork (fragmen rantai yang tidak sah) terdeteksi dan dibongkar dengan memeriksa kompleksitas kumulatif rantai yang disimpan di setiap fork.



PRIZM

PARAMINING

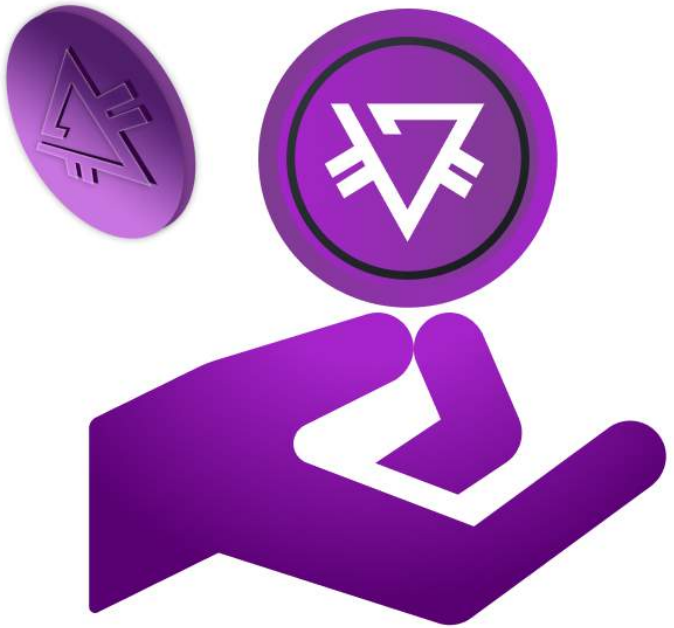
PARAMINING - adalah keunggulan utama PRIZM dibandingkan mata uang kripto lainnya. Pengembang PRIZM menambahkan mekanisme linier-retrograde yang unik untuk menentukan hadiah untuk penyimpanan dana yang ditujukan untuk daya tarik ekonomi dan penggantian bertahap semua instrumen keuangan dunia yang ada oleh massa PZM ke mekanisme dasar pembentukan.

Merupakan tambahan untuk mekanisme penempaan dasar, yang tidak menambah jumlah dana dalam sistem. Dalam PZM ada mekanisme tambahan yaitu ParaMining, yang menciptakan koin baru, menurut metrik pengembangan matematika standar sistem keuangan yang dinormalisasi dalam irisan ekonomi dunia. Menurut perhitungan kami, hanya format pertumbuhan berat koin yang dapat memberikan penggantian secara bertahap dan dengan percaya diri dibanding semua instrumen ekonomi yang ada.

PRIZM

PARAMINING

Tingkat penambangan koin baru menggunakan ParaMining dihitung dari tiga parameter utama,yang mana ini adalah jumlah koin dalam dompet pribadi, jumlah koin dalam dompet pengikut hingga 88 level, dan faktor kesulitan penambangan. Faktor kesulitan dihitung sebagai persentase, dan sebanding dengan jumlah total koin yang dikeluarkan. Level kesulitan maksimum untuk akun standar adalah **98%**, yang sesuai dengan 3 miliar PZM yang dihasilkan. Untuk akun dalam **HOLD - MODE**, kesulitan maksimumnya adalah **97%**. Menurut karakteristiknya, Paramining adalah sistem MLM 2.0 yang mengecualikan segala sesuatu yang mendorong orang sederhana dari bisnis jaringan, tetapi pada saat yang sama melibatkannya dalam pengembangan jaringan untuk meningkatkan kecepatan penambangan koin di dompet pribadinya.



Saat melakukan transaksi apa pun di dompet, sistem ParaMining menulis blockchain yang berisi nilai jumlah koin pemilik dompet dan jumlah koin dalam dompet pengikutnya, saat ini koin baru dihasilkan ke saldo dompet.

«HOLD» - menyimpan koin di dompet pribadi Anda dan tidak melakukan transaksi, karena ini, Anda dapat mengurangi koefisien kesulitan dalam menambang koin dan meningkatkan profitabilitas dompet Anda.

HOLD

PRIZM

PARAMINING

SISTEM PARAMINING adalah alat paling canggih untuk promosi dan popularisasi, karena tidak memiliki analog dalam mata uang kripto modern. Keuntungan utama dari Paramining adalah bahwa tidak ada pengguna jaringan yang dapat mengganggu mekanisme ini dan memalsukan koin baru, semua pengguna dapat memantau jumlah koin yang dikeluarkan oleh sistem. Paramining berfungsi pada dompet apa pun dengan saldo lebih dari 1 PZM dan otomatis berhenti ketika saldo 1 juta PZM tercapai.

Juga untuk pertama kalinya, sistem membangun tautan rujukan tanpa menggunakan tautan apa pun yang diterapkan. Setelah membuat dompet baru, sistem menangkap di blockchain dari siapa transaksi pertama tiba dan secara permanen membangun rantai rujukan yang tidak dapat diubah, ini membuatnya mudah untuk membangun jaringan MLM global dan meningkatkan kecepatan penambangan koin baru.

Implementasi teknis saat ini tidak dijelaskan secara rinci karena faktanya bagi kita semua, yang utama adalah menciptakan bukan 100 alat "mati", tetapi satu dengan dukungan yang baik dan kerja yang baik. Jika pengetahuan kita terungkap, maka seseorang pasti akan mencoba mengulanginya dan ini secara tidak sengaja akan menyebabkan banyak perhatian dan penggunaan ide ini bukan untuk tujuan mulia dan signifikan bagi planet kita, tetapi untuk tujuan yang tidak kita tahu dan tidak selalu berniat positif.

P R I Z M

Untuk mulai menambang PZM baru, cukup diperlukan satu dompet elektronik koin yang secara otomatis memulai ParaMining. Ini adalah proses yang memungkinkan Anda untuk menambah jumlah koin di dompet tanpa biaya listrik.

Paramining dimulai dengan 1 koin dan berhenti secara otomatis ketika Anda mencapai 1 juta koin di dompet Anda.

PILIHAN PARAMINING

Paramaning - adalah metode unik untuk membuat koin baru oleh semua pengguna secara bersamaan, diatur oleh tiga parameter:

1 - Jumlah koin di dompet pribadi Anda
2 - Jumlah koin dari struktur pengikut
3 - Kesulitan menambang bernama Paratax

1 - Jumlah koin di dompet pribadi Anda

Jumlah koin dalam dompet pribadi (PZM)	Keuntungan harian	Keuntungan bulanan
dari 500.000 sampai 1.000.000	0,33%	9,9%
dari 100.000 sampai 499.999	0,28%	8,4%
dari 50.000 sampai 99.999	0,25%	7,5%
dari 10.000 sampai 49.999	0,21%	6,3%
dari 1.000 sampai 9.999	0,18%	5,4%
dari 100 sampai 999	0,14%	4,2%
dari1 sampai 99	0,12%	3,6%

2 - Jumlah koin dari struktur pengikut

Total Volume	Pengganda
dari 1000 sampai 9999	2.18
dari 10.000 sampai 99.999	2.36
dari 100.000 sampai 999.999	2.77
dari 1.000.000 sampai 9.999.999	3.05
dari 10.000.000 sampai 99.999.999	3.36
dari 100.000.000 sampai 999.999.999	3.88
1.000.000.000	4.37

Prinsip Paramining didasarkan pada hukum dasar fisika, dari bagian "Visible Radiation". Seperti model Alam Semesta kita, sistem ini terus berkembang, memperoleh kecepatan, berkat penghitungan ulang yang rumit dengan periode 55 detik.

PRIZM

PILIHAN PARAMINING

Setiap pengguna dengan saldo

dari 1000 sampai 110 000 PZM

dapat meningkatkan periode untuk menghitung bunga majemuk, asalkan saldo terlibat dalam menempa. Untuk memulai periode **HOLD**, Anda harus menghasilkan setidaknya satu blok dengan target transaksi. Periode **HOLD** tidak dapat terganggu oleh transaksi masuk atau dengan menerima biaya penempaan. Durasi periode **HOLD** tidak terbatas, asalkan pemalsu menghasilkan setidaknya satu blok dari **100.000.**

Periode HOLD terganggu oleh transaksi keluar.

PRIZM

PILIHAN PARAMINING

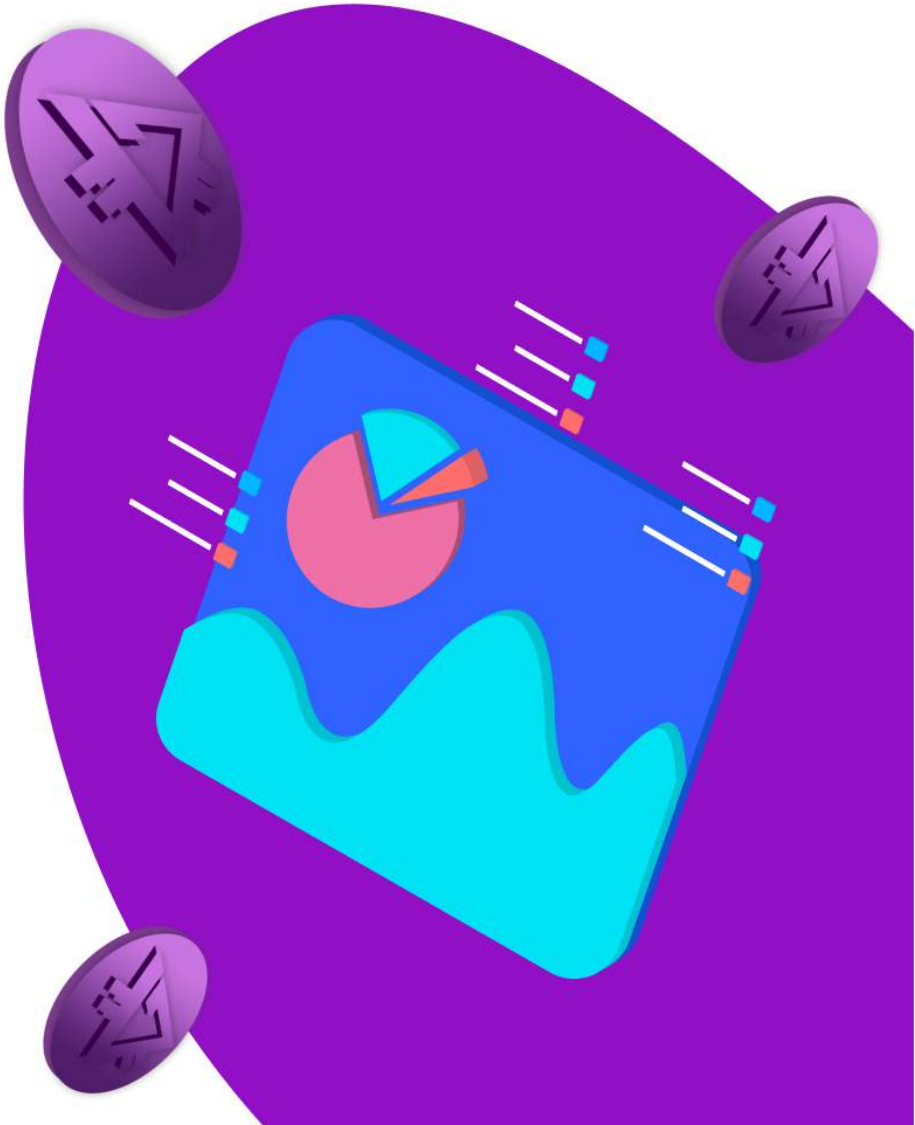
Kesulitan menambang

PARATAX

adalah peningkatan linear dalam kesulitan menghasilkan koin, dinyatakan sebagai persentase dari jumlah koin yang sudah ditambang oleh semua pengguna.

Batas maksimum PARATAX akan menjadi **98%** pada saat produksi 3 miliar PZM.

Untuk **FORGERS** yang saldo pada saat menghasilkan blok tidak melebihi **110.000 PZM**, nilai maksimum PARATAX adalah **97%**

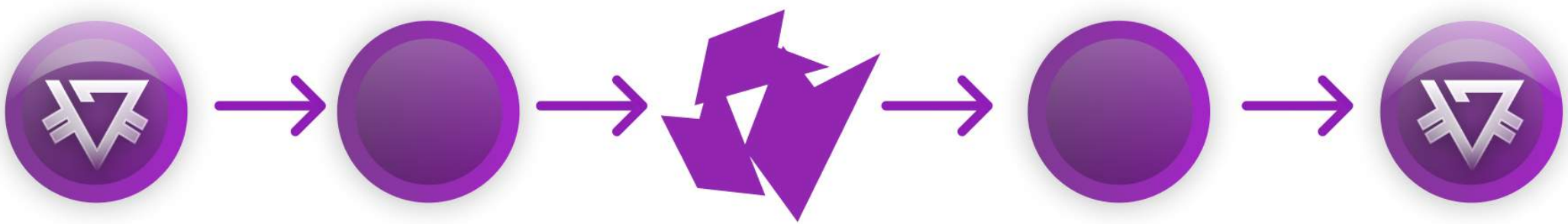


PRIZM

AKUN PRIZM

Prizm mengimplementasikan dompet pintar sebagai bagian dari desainnya: semua akun disimpan di jaringan dengan kunci pribadi untuk setiap alamat akun, langsung diturunkan dari frasa kode setiap akun menggunakan kombinasi operasi SHA256 dan Curve25519. Setiap akun diwakili oleh nomor 64-bit, dan nomor ini dinyatakan sebagai alamat akun menggunakan Kode Solomon untuk Koreksi kesalahan, yang memungkinkan Anda mendeteksi hingga empat kesalahan dalam alamat akun atau memperbaiki hingga dua kesalahan. Format ini diterapkan sebagai tanggapan terhadap kekhawatiran bahwa alamat akun yang salah dapat menghasilkan koin, alias, atau aset yang ditransfer secara permanen ke akun target yang salah.

Alamat akun selalu didahului dengan "PRIZM -", yang membuat alamat akun Prizm mudah dikenali dan berbeda dari format alamat yang digunakan oleh mata uang kripto lainnya.



Alamat akun, kode Solomon-Code yang terkait dengan frasa sandi rahasia dihasilkan dengan cara berikut:

- Frasa sandi rahasia di-hash menggunakan SHA256 untuk mengambil kunci pribadi akun.
- Kunci pribadi dienkripsi menggunakan Curve25519 untuk mendapatkan kunci publik akun.
- Kunci publik di hash dengan SHA256 untuk mendapatkan ID akun.
- 64 bit pertama dari ID akun adalah nomor akun yang terlihat.
- Pengkodean Solomon-Code, nomor akun yang terlihat dengan awalan "PRIZM -" menghasilkan alamat akun.

Ketika sebuah akun diakses dengan frasa sandi rahasia untuk pertama kalinya, itu tidak dilindungi oleh kunci publik. Ketika transaksi keluar pertama kali dilakukan dari akun, kunci publik 256-bit yang diterima dari frasa sandi disimpan di blockchain, dan ini melindungi akun. Ruang alamat untuk kunci publik (2256) lebih besar dari ruang alamat untuk nomor akun (264), jadi tidak ada satu per satu pencocokan kata kode ke nomor akun dan kemungkinan ketidakcocokan. Ketidakcocokan ini terdeteksi dan dicegah sebagai berikut: setelah frasa sandi tertentu digunakan untuk mengakses akun, dan akun dilindungi dengan kunci publik 256-bit, tidak ada pasangan kunci publik-swasta lainnya yang dapat mengakses nomor akun ini.

Properti saldo akun :

1. Saldo akun yang efektif digunakan sebagai dasar untuk mengajukan akun Anda. Saldo akun yang efektif terdiri dari semua koin yang ada dalam akun itu untuk 1.440 blok. Selain itu, fungsi "Leasing akun" memungkinkan Anda untuk mengatur saldo efektif pada akun lain untuk sementara.

2. Saldo akun yang dijamin terdiri dari semua token yang stasioner pada akun untuk 1440 unit. Tidak seperti neraca yang efisien, saldo ini tidak dapat dialihkan ke akun lain mana pun.

3. Saldo akun dasar untuk semua transaksi yang memiliki setidaknya satu konfirmasi.
Saldo akun penambah menunjukkan jumlah total PZM yang diterima sebagai hasil dari penempaan blok yang berhasil.

4. Saldo akun yang belum dikonfirmasi adalah yang ditampilkan di klien Prizm. Ini mewakili saldo akun saat ini, setelah dikurangi koin yang terlibat dalam transaksi yang belum dikonfirmasi dan dikirim.

5. Daftar saldo aset yang dijamin (membuat daftar) , menjamin semua aset saldo yang terkait dengan akun tertentu.

6. Saldo yang belum dikonfirmasi dan daftar saldo aset yang belum dikonfirmasi dari semua aset yang terkait dengan akun tertentu.

PRIZM

WALLET.DAT

Bitcoin dan mata uang terkait sering menggunakan file terenkripsi, dengan nama dan dompet, untuk menyimpan alamat yang dihasilkan untuk menerima koin. Inti berikutnya yang digunakan dalam Prizm tidak juga mensimulasikan fungsi ini, tetapi tidak juga mengesampingkannya. Pengembang klien dapat menerapkan sistem di mana grup kunci pribadi untuk akun Prizm disimpan dalam file yang berdiri sendiri yang dienkripsi.

Konfirmasi transaksi

Semua transaksi PZM dianggap tidak dikonfirmasi hingga dimasukkan dalam blok jaringan yang valid. Blok yang baru dibuat didistribusikan ke jaringan oleh simpul (dan akun terkait) yang membuatnya, dan transaksi yang termasuk dalam blok dianggap sebagai satu konfirmasi yang diterima. Karena blok selanjutnya ditambahkan ke blockchain yang ada, setiap blok tambahan menambahkan konfirmasi lain ke jumlah konfirmasi transaksi. Jika suatu transaksi tidak termasuk dalam blok sebelum kedaluwarsa, ia terbakar dan dihapus dari kumpulan transaksi.

Waktu transaksi

Setiap transaksi mengandung parameter dengan batas waktu yang ditetapkan ke jumlah menit sejak transaksi dikirim ke jaringan. Secara standar, batas waktu adalah 1440 menit (24 jam). Transaksi yang dikirim ke jaringan tetapi tidak termasuk dalam blok disebut transaksi yang belum dikonfirmasi.

Jika transaksi tidak dimasukkan dalam blok sebelum batas waktu transaksi, transaksi dihapus dari jaringan. Transaksi yang dibiarkan tidak dikonfirmasi karena tidak valid atau terdistorsi, atau karena blok diisi dengan transaksi yang menawarkan untuk membayar Komisi yang lebih tinggi. Di masa depan, fitur-fitur seperti transaksi multi-signature(banyak tanda) dapat menggunakan batas waktu sebagai cara melaksanakan kadaluwarsa.

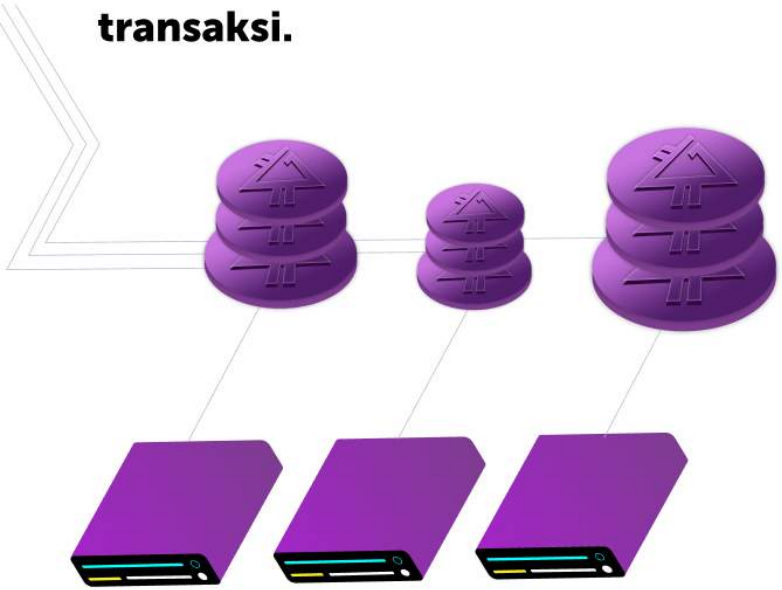
PRIZM

WALLET.DAT

Membuat dan memproses transaksi

Informasi terperinci tentang membuat dan memproses transaksi PZM adalah sebagai berikut:

- Pengirim menentukan parameter transaksi.



Jenis transaksi berubah, dan Anda menentukan jenis yang diinginkan ketika Anda membuat transaksi, tetapi untuk semua transaksi Anda harus menentukan beberapa parameter.

- Kunci pribadi untuk akun pengirim

- Batas waktu transaksi

- Pilihan referensi transaksi

Pertukaran kunci dalam Prizm didasarkan pada algoritma Curve25519, yang menghasilkan rahasia yang dibagikan menggunakan kurva eliptik Diffie-Hellman yang cepat dan efisien dengan tingkat perlindungan yang tinggi. Algoritma ini pertama kali ditunjukkan oleh Daniel J. Bernstein pada tahun 2006. Implementasi Java berikutnya ditinjau oleh Doctor Evil pada Maret 2014. Tanda pada pesan di Prizm dilakukan menggunakan algoritma tanda digital Elliptic-Curve (EC-KCDSA), yang didefinisikan oleh kelompok IEEE P1363a pada tahun 1998 oleh tim percepatan tugas KCDSA. Kedua algoritma dipilih untuk menyeimbangkan kecepatan dan keamanan untuk ukuran kunci hanya 32 byte.

Fitur utama

Klien JavaScript tingkat lanjut

Aplikasi klien yang nyaman dari generasi kedua yang tertanam dalam distribusi perangkat lunak dasar Prizm , dan dapat diakses melalui browser web lokal. Klien memberikan dukungan penuh untuk semua fitur Prizm utama yang diterapkan sehingga kunci pribadi pengguna tidak pernah tersedia online. Ini juga mencakup terhubungnya administratif yang disempurnakan dan membangun dokumentasi Javadoc bawaan untuk menghubungkan pemrograman aplikasi prioritas rendah Prizm.

PRIZM

DASAR-DASAR KRIPTOGRAFI PRIZM

Perangkat portabel

Berkat platform silang pada sumber dasar Java, hashing Proof of Stake(menambang dengan menyimpan koin pada dompet) dan kemampuannya di masa depan untuk mengurangi ukuran rantai blok, Prizm sangat cocok untuk digunakan pada perangkat kecil, sumber daya rendah, daya rendah. Aplikasi dan perangkat lunak Android dan iPhone telah diangkut ke perangkat ARM berdaya rendah seperti platform RaspberryPi dan CubieTruck. Kemampuan untuk menerapkan Prizm pada perangkat berdaya rendah dan selalu terhubung seperti smartphone memungkinkan kami menghadirkan skenario di mana sebagian besar jaringan Prizm didukung pada perangkat seluler. Biaya rendah dan konsumsi sumber daya dari perangkat ini secara signifikan mengurangi biaya jaringan dibandingkan dengan mata uang kripto Proof of Work(menambang menggunakan alat) tradisional.

Pembayaran dasar

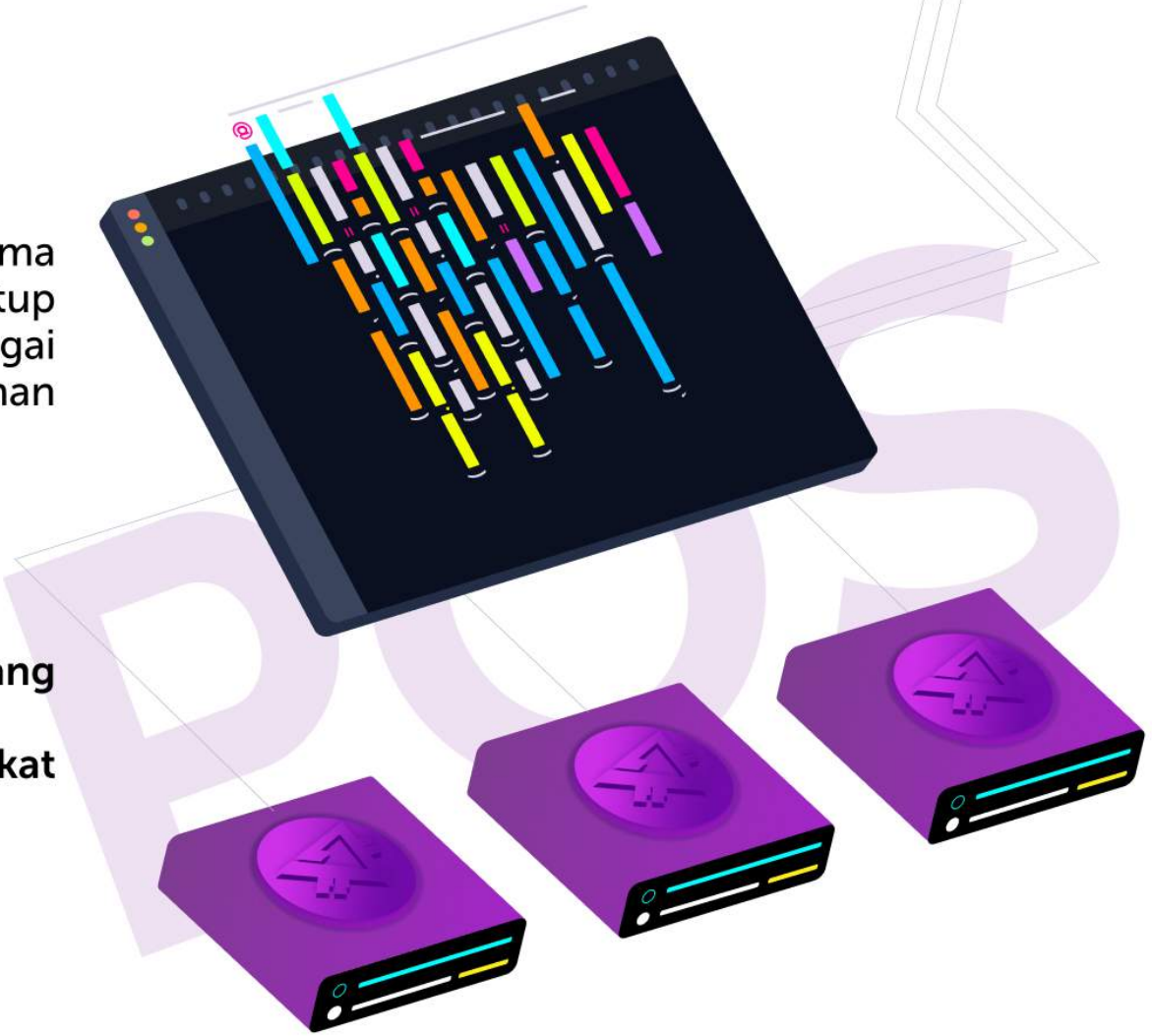
Fitur paling mendasar dari mata uang kripto adalah kemampuan untuk mentransfer koin dari satu akun ke akun lainnya. Ini adalah jenis transaksi Prizm yang paling mendasar, dan memungkinkan Anda untuk menggunakan fungsi pembayaran dasar.

PRIZM

FITUR KUNCI PRIZM

POS-Penempaan

Menggabungkan dua teknologi di waktu yang sama : Paramining + penempaan. Kode sumber ditutup (tidak dibatasi), hingga waktu tertentu, sebagai perlindungan terhadap klon, sebagai jaminan bahwa sistem akan cair.



Program kemitraan dari 88 level dalam struktur
Berikutnya / Inti proof of stake(menambang dengan menyimpan koin) dari sistem kripto
Mudah digunakan serta terhubung ke perangkat seluler
Kata sandi pengguna tidak dikirim ke server

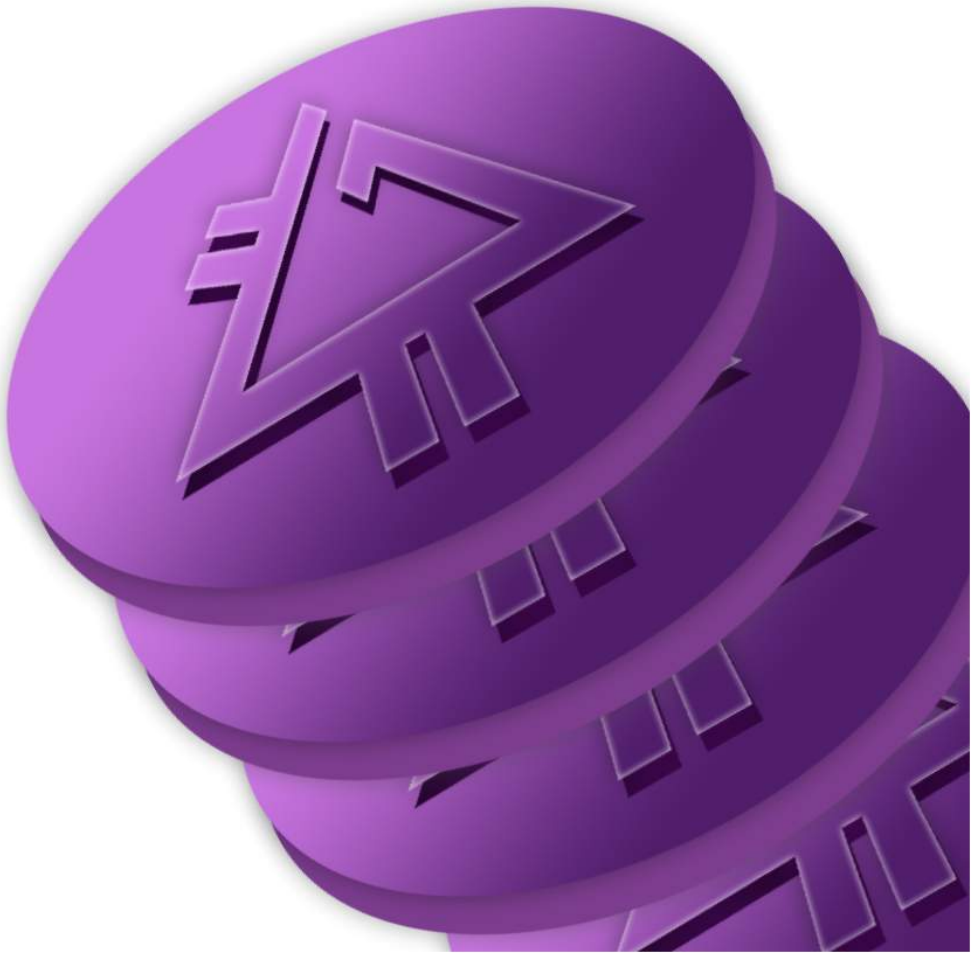
Nothing at stake

Dalam serangan "Nothing at stake", pemalsu mencoba membangun blok di atas semua fork yang mereka lihat karena hampir tidak ada biaya, dan karena mengabaikan fork dapat berarti kehilangan hadiah pada blok yang akan diperoleh jika fork itu dirancang untuk menjadi rantai dengan kesulitan paling kumulatif. Meskipun serangan ini secara teori memungkinkan, saat ini tidak berguna. Jaringan Prizm tidak mengalami blockchain fork yang panjang, dan hadiah untuk blok rendah tidak memberikan banyak dorongan untuk keuntungan; Selain itu, mengkompromikan keamanan jaringan dan kepercayaan untuk keuntungan sekecil itu dapat membuat kemenangan yang banyak memakan korban.

Attack on history

Dalam "attack on history," seseorang memperoleh sejumlah besar koin, menjualnya, dan kemudian mencoba membuat fork yang sukses tepat sebelum koin mereka dijual atau ditukar. Jika serangan gagal, upaya itu tidak ada gunanya karena koin sudah dijual atau ditransfer; Jika serangan berhasil, penyerang mendapatkan tokennya kembali. Bentuk ekstrim dari serangan ini termasuk mendapatkan kunci pribadi dari akun lama dan menggunakannya untuk membangun rantai yang sukses langsung dari blok Genesis. Dalam Prizms, attack on history biasanya gagal karena semua taruhan harus diperbaiki pada 1.440 blok sebelum dapat digunakan untuk menempa; Selain itu, saldo akun efektif yang dihasilkan setiap blok diverifikasi sebagai bagian dari pemeriksaan blok. Bentuk ekstrim dari serangan ini biasanya gagal karena blockchain PRIZM tidak dapat ditata ulang oleh lebih dari 720 blok di belakang tinggi blok saat ini. Ini membatasi jangka waktu di mana aktor yang buruk dapat membentuk serangan ini.

APLIKASI



Masalah Bitcoin, dipertimbangkan dalam Prizm.

Prizm dibuat sebagai mata uang kripto 2.0 - respons terhadap Bitcoin. Prizm menggunakan fungsi yang sudah mapan dalam Bitcoin, dan mempertimbangkan aspek-aspek yang menjadi perhatian. Aplikasi ini membahas masalah dengan Protokol Bitcoin dan jaringan yang dihaluskan oleh teknologi Prizm.

Tentang transaksi per hari

Pada akhir 2013, jumlah transaksi yang diproses dalam jaringan Bitcoin mencapai maksimum 70.000 per hari, yaitu sekitar 0,8 transaksi per detik (tps). Ukuran blok Bitcoin standar saat ini sebesar satu megabyte, dihasilkan (rata-rata) setiap sepuluh menit di situs "penuh" pelanggan, membatasi bandwidth maksimum jaringan Bitcoin yang ada menjadi sekitar 7 TPS. Bandingkan ini dengan bandwidth jaringan VISA untuk menangani 10.000 TPS, dan Anda akan melihat bahwa Bitcoin tidak dapat bersaing seperti yang ada saat ini.

Ukuran Blockchain

Blockchain Bitcoin adalah kumpulan sekuensial lengkap dari blok data yang dihasilkan yang berisi e-book mendaftarkan semua transaksi Bitcoin yang telah terjadi sejak diluncurkan pada Januari 2009. Empat tahun kemudian, pada Januari 2013, ukuran blockchain Bitcoin adalah 4 gigabytes (GB) - perkiraan jumlah data yang diperlukan untuk menyimpan film dua jam di DVD. Delapan belas bulan kemudian, pada bulan Juli 2014, ukuran blockchain Bitcoin meningkat hampir lima hingga 19 gigabytes (GB) 37. Blockchain Bitcoin sedang mengalami pertumbuhan eksponensial, dan modifikasi pada Protokol Bitcoin asli akan memerlukan solusi untuk ini.

Jawaban Prizm

Dalam kondisi saat ini, Prizm dapat menangani hingga 367.200 transaksi per hari - lebih dari sembilan kali puncak Bitcoin saat ini. Implementasi Transparent Forging memungkinkan transaksi diproses hampir secara instan, secara signifikan meningkatkan batas ini.

Saatnya mengkonfirmasi transaksi

Waktu konfirmasi transaksi Bitcoin berkisar antara 5 hingga 10 menit sebagian besar selama 2013. Setelah pengumuman pada akhir 2013 bahwa bank-bank Cina tidak menerima proses Bitcoin, rata-rata waktu transaksi Bitcoin meningkat secara signifikan, menjadi 8-13 menit , dengan puncak periode 19 menit. Sejak itu, waktu konfirmasi telah bergeser dari 8 menjadi 10 menit. Namun, karena beberapa cek (biasanya enam konfirmasi) diperlukan untuk menyelesaikan transaksi Bitcoin, satu jam dapat dengan mudah berlalu sebelum penjualan aset yang dibayar oleh Bitcoin selesai.

Jawaban PRIZM

Waktu rata-rata pembuatan blok PZM pada riwayat telah terbukti sekitar 80 detik, dan waktu pemrosesan transaksi rata-rata adalah sama. Transaksi dianggap aman setelah sepuluh konfirmasi, yang berarti bahwa transaksi menjadi permanen dalam waktu kurang dari 14 menit. Penerapan Transparent Forging memungkinkan Anda melakukan transaksi yang hampir instan, yang akan semakin mengurangi waktu ini

Masalah sentralisasi

Peningkatan kompleks bersama dengan tingkat hash untuk Bitcoin telah menciptakan penghalang yang tinggi untuk masuk bagi pendatang baru, dan keuntungan yang lebih rendah untuk instalasi penambangan yang ada. Insentif untuk mendorong blok yang digunakan oleh Bitcoin telah menyebabkan terciptanya instalasi besar tingkat tunggal dari peralatan penambangan khusus 44, serta ketergantungan pada sekelompok kecil kolam penambangan besar 45. Hal ini menyebabkan efek "sentralisasi", di mana Penambangan dalam jumlah besar terkonsentrasi pada kontrol jumlah orang yang semakin berkurang. Ini tidak hanya menciptakan jenis struktur kekuatan yang dirancang Bitcoin untuk memotong, tetapi juga menghadirkan kemungkinan nyata bahwa satu operasi penambangan atau gabungan dapat memperoleh 51% dari total kapasitas penambangan di jaringan 46 dan melakukan serangan 51% . Ada juga serangan yang hanya membutuhkan 25% dari total daya hashing jaringan. Pada awal Januari 2014 GHash.io mulai secara sukarela mengurangi kekuatan penambangannya sendiri, karena mendekati level 51%. Beberapa hari kemudian, kekuatan di kolam menurun menjadi 34% dari total kapasitas jaringan, tetapi kecepatannya segera mulai meningkat, dan pada Juni 2014 kembali mencapai tingkat berbahaya.

Jawaban PRIZM

Insentif yang diberikan oleh algoritma Proof of Stake(menambang dengan menyimpan koin dalam dompet) yang digunakan dalam Prizm memberikan pengembalian investasi yang rendah sekitar 0,1%. Karena koin baru tidak dihasilkan setiap blok, tidak ada "hadiah untuk penambangan" tambahan, yang mendorong upaya bersama untuk membuat blok. Data menunjukkan bahwa jaringan Prizm tetap sangat terdesentralisasi sejak awal: besar (dan terus bertambah) jumlah akun unik menambah blok ke jaringan.

Proof of Work(menambang menggunakan alat) - biaya pemeliharaan

Konfirmasi transaksi pada bitcoin yang ada dan membuat bitcoin baru yang masuk ke sirkulasi membutuhkan daya komputasi yang sangat besar, yang harus bekerja terus-menerus. Kekuatan komputasi ini disediakan oleh rig penambangan yang disebut, yang dikelola oleh penambang. Penambang Bitcoin bersaing satu sama lain untuk menambahkan blok transaksi berikutnya ke rantai bitcoin keseluruhan. Ini dilakukan dengan "hashing" - menggabungkan semua transaksi Bitcoin yang terjadi dalam sepuluh menit terakhir, dan mencoba mengenkripsi mereka menjadi blok data, yang juga secara kebetulan memiliki sejumlah nol berturut-turut di dalamnya. Sebagian besar blok percobaan yang dihasilkan oleh hashing miner tidak memiliki jumlah target nol ini, sehingga mereka membuat perubahan kecil dan mencoba lagi. Satu miliar upaya untuk menemukan blok "menang" ini disebut GH, dan rig penambangan diperkirakan dengan berapa banyak GH yang dapat dilakukannya per detik, dilambangkan dengan GH / detik. Penambang yang menang, yang merupakan orang pertama yang menciptakan blok Bitcoin yang benar secara kriptologis, segera menerima hadiah 25 bitcoin baru - hadiah pada saat penulisan adalah sekitar 15 750 dolar AS. Persaingan antara penambang dengan penghargaan ini diulang-ulang setiap sepuluh menit sekali. Pada awal 2014, lebih dari 3.500 bitcoin per hari, setara dengan sekitar $ 2,2 juta per hari, telah dihasilkan. Dengan begitu banyak uang pada taruhan, para penambang mendukung perlombaan senjata cepat dalam teknologi rig pertambangan untuk meningkatkan peluang mereka untuk menang. Awalnya, bitcoin ditambang menggunakan prosesor Central (CPU), komputer desktop biasa. Kemudian untuk meningkatkan kecepatan chip dari unit pemrosesan grafis khusus (GPU) dalam kartu grafis kelas atas digunakan. Kemudian mikroprosesor dengan array gerbang yang dapat diprogram (FPGA) dan kemudian chip sirkuit terintegrasi terapan khusus (ASIC) digunakan. Teknologi ASIC adalah puncak dari garis untuk penambang bitcoin, tetapi perlombaan senjata terus berlanjut dengan munculnya generasi berbeda dari chip ASIC.

Proof of Work(menambang menggunakan alat) - biaya pemeliharaan

Generasi terkini dari chip ASIC adalah apa yang disebut perangkat 28 nm berdasarkan ukuran transistor mikroskopis mereka dalam nanometer. Mereka harus diganti dengan modul ASIC 20nm pada akhir 2014. Contoh keadaan baru dari rig penambangan seni akan menjadi kartu ASIC 28nm "Raja" dari Butterfly Labs, yang menyediakan 600GH / detik untuk konsumsi listrik 350 watt dan harga 2.200 USD. Infrastruktur rig penambangan, yang saat ini digunakan untuk mendukung operasi Bitcoin saat ini, sangat mengejutkan. Bitcoin ASIC mirip dengan ilmuwan - mereka hanya dapat melakukan perhitungan satu blok bitcoin dan tidak lebih, tetapi mereka dapat melakukannya dengan satu perhitungan dengan kecepatan super komputer. Pada November 2013, majalah Forbes menerbitkan sebuah artikel berjudul "kekuatan komputasi bitcoin global 256 kali lebih cepat dari 500 super komputer gabungan!". Pada pertengahan Januari 2014, statistik yang disimpan di situs blockchain.info, menunjukkan bahwa dukungan terus menerus dari operasi Bitcoin membutuhkan tingkat hash berkelanjutan sekitar 18 juta GH / detik. Dalam satu hari, kekuatan hashing ini menghasilkan 1,5 triliun blok uji coba, yang dihasilkan dan ditolak oleh Bitcoin, untuk mencari satu - 144 blok ajaib yang akan mencakup mereka $ 2,2 juta. Hampir semua perhitungan Bitcoin tidak ditujukan untuk memperbaiki bencana dengan memodelkan DNA atau mencari sinyal radio dari E. T .; Sebaliknya, mereka benar-benar sia-sia. Kekuatan dan biaya yang terkait dengan dukungan latar belakang Bitcoin yang boros ini sangat besar. Jika semua rig penambangan Bitcoin memiliki level "Raja", seperti dijelaskan di atas - dan tidak akan sampai mereka ditingkatkan - mereka akan mewakili kumpulan 30.000 mesin yang bernilai lebih dari $ 63 juta. Itu mengkonsumsi lebih dari 10 mega watt daya terus menerus selama operasi dan tagihan listrik lebih dari $ 3,5 juta per hari. Angka sebenarnya jauh lebih tinggi untuk kumpulan mesin rig penambangan saat ini yang kurang efisien yang sebenarnya mendukung Bitcoin saat ini. Dan angka-angka ini sekarang naik kurva pertumbuhan eksponensial sebagai bitcoin berbaris dari satu transaksi saat ini per detik ke maksimum saat ini tujuh transaksi per detik.

Solusi Prizm

Analisis biaya dan efisiensi energi dari jaringan Prizm menunjukkan bahwa seluruh ekosistem PRIZM dapat dipertahankan sekitar $ 60.000 per tahun, yang sekarang hampir 2.200 kali lebih murah daripada biaya pengoperasian jaringan Bitcoin.

PRIZM.SPACE

Biaya pemeliharaan POW terkait dengan pemegang koin

Selain biaya listrik yang sangat besar, ada biaya tersembunyi untuk penyimpanan bitcoin yang sederhana. Untuk setiap blok yang ditemukan, orang yang menghasilkan blok menerima hadiah. Pada saat penulisan, kurang lebih 12,5 BTC hadiah(untuk sekarang), yang merupakan inflasi 10% dari total pasokan Bitcoin tahun ini. Untuk setiap $ 1.000 bitcoin miliknya, orang ini membayar $ 100 bitcoin untuk "membayar" penambang sebagai keamanan jaringan.

Semoga mempercepat langkahmu

Integrasi PRIZM

Sistem pembayaran PRIZM adalah cara termudah untuk menerima dan mengirim pembayaran kripto.

Anda dapat dengan mudah mengintegrasikan PRIZM ke proyek, toko online, penukaran, dan lain-lain

Pengajaran online :

https://pzm.space/en/pzm-integration/

Untuk memulai bekerja dengan PRIZM, Anda harus meluncurkan simpul jaringan (Node) dan API_Servlet.

Perangkat lunak ini dapat berjalan di satu server maupun di server yang berbeda. Namun lebih baik berjalan di satu server untuk kenyamanan Anda.

Pertama, Anda harus meluncurkan node dan tunggu selagi sinkronisasi. Langkah selanjutnya adalah konfigurasi modul **PrizmAPIServlet**.

Integrasi sistem pembayaran Prizm

Simpul Jaringan

PrizmCore wallet
https://github.com/prizmspace/PrizmCore#prizmcore-wallet-download-v1103-windows-osx-linux

Easy API Gateway
https://github.com/prizmspace/PrizmCore#easy-api-gateway-prizmapiservlet

Konfigurasi PrizmAPIServlet

Dalam arsip ada file bernama :

PrizmAPIServlet.properties

Setelah Anda mengisi kolom, Anda harus meluncurkan servlet melalui

run-servlet.sh

dalam barisan

frasa sandi: NONE

sebagai ganti NONE, Anda harus menulis kunci pribadi dompet yang akan digunakan oleh proyek Anda.

dalam barisan

kunci mengirim: NONE

sebagai ganti NONE, Anda harus menulis kata sandi (itu akan digunakan oleh fungsi pengiriman koin sebagai perlindungan tambahan dari transaksi yang tidak sah).

Contoh implementasi dalam PHP

Deskripsi pekerjaan dengan menerima dan mengirim koin, dengan contoh fungsi siap pakai dan deskripsi prinsip kerja. Database Mysql digunakan untuk menyimpan daftar transaksi, ada dump dari tabel penyimpanan di bawah ini, bersama dengan contoh kode untuk bekerja dengan tabel (jika Anda menerapkan QueryBuilder, itu tidak akan menjadi masalah).

Prinsip kerja utama:

Ada skrip dalam tugas Cron yang membuat permintaan ke servlet setiap 2-5 menit sehingga bisa menerima transaksi baru di dompet penyimpanan. Setelah menerima daftar transaksi, Anda harus menyimpannya ke database lokal. Jika tidak ada operasi dalam database, Anda harus menjalankan perintah tanpa parameter apa pun. Namun jika Anda ingin menerima transaksi baru, Anda harus mengirim nomor transaksi terakhir yang Anda miliki sebagai parameter.

Contoh dari fungsi:

```
<?php
function historyPZM($last_id = 0)
{
 if ($last_id) {
  $url = 'http://localhost:8888/history?fromid=' . $last_id;
 } else {
  $url = 'http://localhost:8888/history';
 }
 $page = '';
 $result = get_web_page($url);
 if (($result['errno'] != 0) || ($result['http_code'] != 200)) {
  $error = $result['errmsg'];
 } else {
  $page = $result['content'];
 }
 $array_new = array();
 $xcmorewrite = explode("\n", str_replace("\r", '', $page));
 foreach ($xcmorewrite as $value) {
  if ($value) {
   $array_new[] = explode(";", $value);
  }
 }
 return $array_new;
}
?>
```

Fungsi untuk mengambil konten halaman:

```php
<?php

function get_web_page($url)
{
 $uagent = "Opera/9.80 (Windows NT 6.1; WOW64) Presto/2.12.388 Version/12.14";
 $ch = curl_init($url);
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1); // memulihkan halaman web
       curl_setopt($ch, CURLOPT_HEADER, 0); // tidak memulihkan tajuk
       curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1); // ikuti arahan ulang
       curl_setopt($ch, CURLOPT_ENCODING, ""); // menangani semua penyandian
      curl_setopt($ch, CURLOPT_USERAGENT, $uagent); // Agen pengguna
      curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, 20); // batas waktu koneksi
      curl_setopt($ch, CURLOPT_TIMEOUT, 20); // batas waktu jawaban
      curl_setopt($ch, CURLOPT_MAXREDIRS, 2); // berhenti setelah pengalihan ke-10

 $content = curl_exec($ch);
 $err = curl_errno($ch);
 $errmsg = curl_error($ch);
 $header = curl_getinfo($ch);
 curl_close($ch);

 $header['errno'] = $err;
 $header['errmsg'] = $errmsg;
 $header['content'] = $content;
 return $header;
}

?>
```

Fungsi untuk mengambil konten halaman:

Anda dapat mengujinya melalui konsol, misalnya: curl http://localhost:8888/history

Contoh skrip penangan tugas Cron untuk menerima transaksi baru dan struktur tabel

```
CREATE TABLE `pzm_history` (
 `id` bigint(20) NOT NULL,
 `tarif_id` int(1) NOT NULL,
 `tr_id` varchar(255) NOT NULL,
 `tr_date` varchar(255) NOT NULL,
 `tr_timestamp` int(11) NOT NULL,
 `pzm` varchar(50) NOT NULL,
 `summa` decimal(16,2) NOT NULL,
 `mess` varchar(255) NOT NULL,
 `status` int(1) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

** Semua kunci dan peningkatan otomatis yang diperlukan untuk ID harus ditambahkan ke tabel

Handler:

Dalam contoh ini Anda menerima daftar transaksi baru yang harus disimpan ke database lokal.

Karena itu, Anda menyimpan riwayat semua transaksi di dompet dan di masa depan Anda akan mencarinya di basis data lokal kami menggunakan data kunci.

```
<?php
$nomer = getLastPrmHistory();
$historys = historyPZM($nomer);

foreach ($historys as $item) {
  if ($item['0'] != "No transactions!") {

// baris ini menambahkan data ke 'pzm_history' menggunakan tabel INSERT IGNORE

PzmHistory::find()->insertIgnore([
        'tr_id' => $item['0'],
        'tr_date' => $item['1'],
        'tr_timestamp' => $item['2'],
        'pzm' => $item['3'],
        'summa' => $item['4'],
        'mess' => $item['5'],
        'status' => 0
    ]);
  }
}
```

```
function getLastPrmHistory()
{
// baris ini mencari baris terakhir dalam tabel untuk mendapatkan ID terakhir dari transaksi yang ada dalam tabel

if (!empty($pzmHistory = PzmHistory::find()->orderBy('id', "DESC")->first())) {
  return $pzmHistory->tr_id;
 };
 return 0;
}

?>
```

Proyek Anda harus bekerja dengan Dompet Prizm yang sama, itu sebabnya semua klien akan diberikan persyaratan yang sama untuk mengisi akun internal dan ID hash yang sama dari operasi. Pastikan untuk memberi tahu klien bahwa ia harus melakukan transaksi secara ketat pada syarat yang menunjukkan pengidentifikasi hash dalam komentar pembayaran.

Dengan demikian, harus ada proses lain yang akan menganalisis transaksi masuk baru dan menyetor koin ke akun internal jika komentar pembayaran memiliki pengenal hash klien. Anda juga perlu membuat tombol "I **PAID**" yang terpisah untuk klien yang dapat mencari dan mencatat transaksi baru untuk pengguna ini setelah melakukan klik padanya.

Fungsi sekunder dan fungsi pengiriman koin

Mendapatkan kunci publik untuk dompet (hanya berfungsi untuk dompet aktif yang memiliki saldo).

```
<?php

 function destinationPZM($pzm)
   {
      $url = 'http://localhost:8888/publickey?destination=' . $pzm;
      $page = '';
      $result = get_web_page($url);
      if (($result['errno'] != 0) || ($result['http_code'] != 200)) {
         $error = $result['errmsg'];
         return '';
      } else {
         $page = $result['content'];
         $haystack = "Public key absent";
         $haystack2 = "Send error!";
         $pos = strripos($page, $haystack);
         $pos2 = strripos($page, $haystack2);
         if ($pos === false AND $pos2 === false) {
            $xcmorewrite = explode(' ', $page);
            $page = trim($xcmorewrite[0]);
            return $page;
         } else {
            return '';
         }
      }
      return $page;
   }

?>
```

Menerima saldo dompet saat ini:

```
<?php

 function getBalancePZM($pzm)
  {
     $ip = '*******';  // contoh 192.168.1.1:9976  dengan port
 $url = 'http://'.$ip.'/prizm?requestType=getAccount&account=' . $pzm;
     $page = '';
     $result = get_web_page($url);
 //print_r($result); die;
     if (($result['errno'] != 0) || ($result['http_code'] != 200)) {
        $error = $result['errmsg'];
        return '';
     } else {
        $page = $result['content'];
        $page = json_decode($page, true);
        if ( isset($page['balanceNQT']) ) {
          return $page['balanceNQT'] / 100;
        } else {
          return 0;
        }
     }
  }

?>
```

Metode pengiriman koin:

```
<?php

public function payPZM($summa, $pzm, $public_key, $text)
{
 $p2 = SENDKEY;      // ini adalah kata sandi yang Anda tentukan selama pengaturan
 $return = false;
 $url = 'http://localhost:8888/send?sendkey=' . $p2 . '&amount=' . $summa . '&comment=' . urlencode($text) . '&destination=' . $pzm . '&publickey=' . $public_key;
 $page = '';
 $result = get_web_page($url);

 if (($result['errno'] != 0) || ($result['http_code'] != 200)) {
  $error = $result['errmsg'];
 } else {
  $page = $result['content'];
 }

 if (preg_match('/^\+?\d+$/', $page)) {
  $return = true;
 } else {
  $return = false;
 }
 return $return;
}

?>
```

LAPORAN RESMI

PRIZM

Konsep awal mata uang digital

Revisi Laporan Resmi

Prizm — June, 2020

PZM.SPACE